

TITLE OF THE INVENTION

COMMUNICATION APPARATUS AND METHOD

5 BACKGROUND OF THE INVENTION

This invention relates to a communication apparatus and method capable of transmitting information to another party by facsimile communication or  
10 communication using electronic mail.

The increasing use of electronic mail over the Internet in recent years has led to the appearance even of facsimile machines that can be connected to the Internet or to a LAN to make possible the sending and  
15 receiving of electronic mail.

Maintaining the security of document information sent and received by facsimile is a concern. Since facsimile communication via an ordinary public telephone network involves a direct one-on-one connection between  
20 the communicating parties via the network, the degree of security in terms of the communication path is comparatively high. However, once the faxed documents have been received by the facsimile machine on the receiving side, the received information is, as a rule, 25 printed out by the receiving facsimile machine. The degree of security on the receiving side, therefore, is

comparatively low.

A solution has been to use a confidential message-box function to assure secrecy. This function involves the sending side notifying the receiving side of the 5 fact that a confidential transmission is to be made, accumulating the received documents in a confidential message box on the receiving side and outputting the documents on the receiving side only when a correct secret number has been entered.

10       Conversely, with regard to electronic mail sent over the Internet, mail arrives at the communicating party on the receiving side via a number of unspecified routers and mail servers, etc., that constitute the network, and ASCII character codes are exchanged over 15 this communication path as is. The degree of security in this case, therefore, is comparatively low. However, because an electronic mail scheme comes equipped with a mailbox function, the degree of security of received documents once they have arrived at the receiving party 20 is high.

Thus, the security of documents communicated by facsimile differs greatly from that communicated by electronic mail. In order to assure an equivalent degree of security for both kinds of communication with 25 the conventional apparatus of the type described above, the user must perform different communication operations

upon being sufficiently aware of the difference in security of both kinds of communication.

#### SUMMARY OF THE INVENTION

5

Accordingly, an object of the present invention is to provide a communication apparatus capable of affording an equivalent level of security for both facsimile transmission and electronic mail without the 10 user needing to be aware of the difference between facsimile transmission and electronic mail.

Another object of the present invention is to afford an equivalent level of security for both facsimile transmission and electronic mail in a case 15 where the user indicates the need for security at the time of document transmission, wherein image data is encrypted if a document is transmitted by an electronic mail function and, if possible, a private security function is used if a document is transmitted by 20 facsimile.

According to the present invention, the foregoing objects are attained by providing a communication apparatus comprising: facsimile communication means for transmitting transmission information to a destination 25 apparatus in accordance with facsimile communication specifications; electronic-mail communication means for

transmitting transmission information to a destination apparatus in accordance with electronic-mail specifications; communication designating means for causing transmission of the transmission information by 5 selecting either the facsimile communication means or the electronic-mail communication means; and security designating means for designating whether the transmission information is confidential information; wherein if the transmission information has been 10 designated as being confidential information by the security designating means, the facsimile communication means transmits the transmission information to the destination apparatus as is by facsimile transmission when the facsimile communication means has been 15 designated by the communication designating means, and the electronic-mail communication means encrypts the transmission information and then sends it to the destination apparatus by electronic mail when the electronic-mail communication means has been designated 20 by the communication designating means.

By way of example, if the destination apparatus possesses a private security function, the facsimile communication means transmits the transmission information to a mailbox utilizing this private security 25 function if the transmission information has been designated as being confidential information by the

security designating means.

Further, the transmission information is, e.g., document information obtained by reading a document.

Other features and advantages of the present  
5 invention will be apparent from the following  
description taken in conjunction with the accompanying  
drawings, in which like reference characters designate  
the same or similar parts throughout the figures  
thereof.

10

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an embodiment according to the present invention; and

15 Fig. 2 is a flowchart illustrating transmission processing according to this embodiment.

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

20 A preferred embodiment of the present invention will now be described in detail with reference to the drawings.

Fig. 1 is a block diagram illustrating the construction of an image-information communication apparatus according to an embodiment of the present  
25 invention.

As shown in Fig. 1, the apparatus includes a CPU 101 for exercising overall control of the apparatus; a ROM 102 for storing the control program; a RAM 103 for storing program control variables and the like; an image memory 104, which is constituted by a DRAM or the like, for storing information such as data that is sent and received.

The apparatus further includes an image reader 105, which includes such components as an image sensor and a document transport mechanism, for optically reading a document and converting it to electrical image data, and a control panel 106 for inputting various operating commands and having an external display unit capable of being implemented by an LCD, LEDs or the like. The external control unit displays the status of the apparatus and the results of commands and thus interfaces the operator.

The apparatus further includes an image recording unit (printer) 107 for printing a received image or file data on printing paper; a LAN interface 108 which exercises control for connecting the apparatus to a LAN 300; and an image format converter 109 for subjecting an image to various format conversions.

The apparatus further includes an electronic-mail format converter 110 for converting text data and image data to an electronic-mail format; an electronic-mail

format analyzer 111 for analyzing the content of data having an electronic-mail format; a public-network interface 112 used to connect the apparatus to a facsimile machine 250 of another party via a public 5 network 200; and an encryption processor 113 for encrypting electronic-mail transmission information under the control of the CPU 101.

The public network 200, which is a public facsimile communications network, is capable of being connected to 10 the other communication apparatus 250 via a public-network interface and can transmit information to the other communication apparatus 250 in accordance with facsimile communication specifications. It should be noted that the other communication apparatus 250 capable 15 of being connected to the public network 200 has a mailbox 260.

The LAN 300 is capable of sending and receiving electronic mail. The apparatus according to this embodiment is adapted so that information can be 20 transmitted between this apparatus and another communication apparatus 350 by electronic mail via the LAN interface 108. Numeral 400 denotes a mail server that is capable of accumulating electronic mail.

Reference will be had to Fig. 2 to describe 25 transmission processing for reading a document image by the image reader 105 and transmitting the image to a

desired destination in accordance with the embodiment having the construction set forth above. Fig. 2 is a flowchart illustrating transmission processing according to this embodiment.

5       A sending party who wishes to transmit a document image using the apparatus of this embodiment first places the document in the image reader 105 and uses the control panel 106 to enter various indications necessary for transmission (step S101). These indications include

10      an indication of the destination to which data is to be communicated, an indication as to whether transmission is a confidential transmission, and an indication of the transmission method, i.e., whether transmission is by facsimile or electronic mail.

15      The sending party commands transmission by entering a command from the control panel 106 to start the scanning of a document. Upon sensing the transmission command, the CPU 101 sends the read document information (transmission information) to the image format converter 109 at step S102. The image format converter 109 encodes this information in accordance with a data format in a case where facsimile communication compliant with the G3 standard, for example, is carried out. The coded transmission information is stored in the image memory 104 at step S103. For example, all documents are stored in the image memory 104.

If the scanning of all documents is finished, then, at step S104, the input state of a key that is for commanding a confidential transmission from the control panel 106 at step 101 is sensed and it is determined 5 whether the command indicates confidential transmission. According to this embodiment, if the command indicates a confidential transmission, it is judged that security needs to be assured at the time of document transmission and data transmission in which security is assured is 10 carried out.

If it is determined at step S104 that the transmission is not confidential, then control proceeds to step S105 and ordinary transmission is performed in accordance with the specified transmission method.

15 More specifically, if a confidential transmission has not been designated, then, at step S105, it is determined whether the designation of the communication method from the control panel 106 is selection of facsimile transmission or selection of transmission by 20 electronic mail. Control proceeds to step S106 in a case where facsimile communication has been selected to transmit data to the transmission destination.

In this case, a telephone number is specified as the destination identifying information. As a result, 25 the CPU 101 starts up the public-network interface 112 to call the public network 200, sends the public network

200 a telephone number signal such as a dial signal or MF signal corresponding to the specified destination telephone number and calls the apparatus of the other communicating party to thereby form a communication path 5 to the destination apparatus. Next, at step S107, the document image data that has been stored in the image memory 104 is transmitted to the destination apparatus by data communication (facsimile communication). Processing is exited when all image data has been 10 transmitted.

If it is found at step S105 that the designation of the transmission method from the control panel 106 is selection of transmission by electronic mail and an electronic mail address has been specified as the 15 destination of communication, then control proceeds to step S110 to start up the image format converter 109. The latter converts the read document information to an image format such as the TIFF-F format. The converted data is then applied to the electronic-mail format 20 converter 110, which applies coding conforming to electronic mail, such as BASE64, to thereby convert the data to information capable of being transmitted as electronic mail.

Next, at step S111, the LAN interface 108 is 25 activated to transmit the information, along with the mail address of the destination and the mail address of

the local apparatus, to the other communication apparatus 350 via the LAN 300. More specifically, the transmission data is transferred from the apparatus of this embodiment to the mail server 400 via the LAN 300, 5 and the other communication apparatus 350 at the destination accepts the data from the mail server 400.

If it is determined at step S104 that the control panel 106 has issued a confidential-transmission command, control proceeds to step S108, where it is 10 determined whether the method of transmission selected at the control panel 106 is transmission based upon electronic mail or facsimile transmission using the public network 200.

If transmission by electronic mail has been 15 selected, control proceeds to step S109, where the encryption processor 113 is activated to encrypt the transmission information that has been stored in the image memory 104. This is followed by the processing from step S110 onward, at which the encrypted 20 information is converted to an image format such as the TIFF-F format by the image format converter 109, then converted to an electronic-mail format by the electronic-mail format converter 110 and transferred to the mail server 400 via the LAN interface 108 and LAN 25 300.

In the example described above, first encryption

processing is executed at step S109 and then a conversion is made to the image format such as TIFF-F. However, the mode of the invention is not limited to the above-described example. By way of example, control may 5 be performed in such a manner that image data is encrypted after a conversion is made to the image format such as TIFF-F. Furthermore, encryption may be performed after a conversion is made to the image format such as TIFF-F. In other words, security can be assured 10 if encryption is performed by the time of transmission to the LAN 300.

If it is found at step S108 that facsimile communication has been selected as the communication method, control proceeds to step S112. Here, through 15 control similar to that of step S106, the public-network interface 112 is started up to call the public network 200, a telephone number signal or the like corresponding to the destination telephone number specified by the control panel 106 is sent to the public network 200 and 20 the desired destination facsimile apparatus, e.g., the other communication apparatus 250, is called to thereby form a communication path to the destination apparatus.

Next, at step S113, processing which precedes well-known facsimile communication processing is executed to 25 determine whether the other communication apparatus supports a private security function. If the other

communication apparatus does not support a private security function, control proceeds to step S107. Here, in a manner similar to that of the usual case described above, the document image data that has been stored in 5 the image memory 104 is sent to the destination apparatus as is and the latter executes processing similar to the usual facsimile communication processing.

If it is found at step S113 that the other apparatus does have a private security function, on the 10 other hand, then control proceeds to step S114. Here the other communication apparatus 250 is notified of the fact that the communication to follow will be a confidential transmission and then the transmission data that has been stored in the image memory 104 is 15 transmitted to the other communication apparatus 250 at the destination via the public-network interface 112 and public network 200. The other communication apparatus 250 performs confidential reception, such as by storing the received information in the mailbox 260, and 20 executes reception processing in accordance with a method that enables security to be assured.

The example described above relates to a case where the apparatus of the embodiment is provided on the transmitting side. However, the apparatus can operate 25 also as an apparatus provided on the receiving side. In such case encrypted data that has been encrypted and

sent when security is required is applied to the encryption processor 113. The latter decodes the data by decryption.

Facsimile data that has been sent by confidential 5 transmission may be stored in a designated mailbox and the designated recipient may be informed of the fact that confidential reception took place.

Thus, in accordance with the embodiment described above, there are provided means for transmitting a 10 document by facsimile, means for transmitting a document as by electronic mail, means for designating which of these two means is to transmit a document, and means for designating whether a document is to be kept confidential. As a result, when confidentiality of a 15 document is designated and transmission by electronic mail is designated at the time of transmission, the document can be transmitted upon being encrypted. Thus, a document can be sent and received safely by an electronic-mail function even in applications where a 20 high level of security is required. Furthermore, facsimile communication can be carried out as well and in this case also a private security function can be used satisfactorily to maintain an equivalent level of security.

25 For example, if an indication for assuring security is made when document information is transmitted, image

data is encrypted in a case where the document is transmitted by an electronic-mail function and the above-mentioned private security function is used in a case where the document is transmitted by facsimile.

5 Thus there can be provided a communication apparatus that is capable of affording an equivalent level of security without the user needing to be aware of the difference between a facsimile transmission and an electronic-mail transmission.

10 The present invention can be applied to a system constituted by a plurality of devices (e.g., a host computer, interface, reader, printer, etc.) or to an apparatus comprising a single device (e.g., a copier or facsimile machine, etc.).

15 Furthermore, it goes without saying that the object of the invention is attained by supplying a storage medium storing the program codes of the software for performing the functions of the foregoing embodiment to a system or an apparatus, reading the program codes with  
20 a computer (e.g., a CPU or MPU) of the system or apparatus from the storage medium, and then executing the program codes.

In this case, the program codes read from the storage medium implement the novel functions of the  
25 invention, and the storage medium storing the program codes constitutes the invention.

Further, the storage medium, such as a floppy disk, hard disk, optical disk, magneto-optical disk, CD-ROM, CD-R, magnetic tape, non-volatile type memory card or ROM can be used to provide the program codes.

5 Furthermore, besides the case where the aforesaid functions according to the embodiment are implemented by executing the program codes read by a computer, it goes without saying that the present invention covers a case where an operating system or the like running on the  
10 computer performs a part of or the entire process in accordance with the designation of program codes and implements the functions according to the embodiments.

It goes without saying that the present invention further covers a case where, after the program codes  
15 read from the storage medium are written in a function expansion board inserted into the computer or in a memory provided in a function expansion unit connected to the computer, a CPU or the like contained in the function expansion board or function expansion unit  
20 performs a part of or the entire process in accordance with the designation of program codes and implements the function of the above embodiment.

In a case where the present invention is applied to the above-mentioned storage medium, program code  
25 corresponding to the flowchart of Fig. 2 described earlier would be stored on the storage medium.

Thus, in accordance with the present invention, as described above, there can be provided a communication apparatus that is capable of affording an equivalent level of security without the user needing to be aware 5 of the difference between a facsimile transmission and an electronic-mail transmission. Specifically, if an indication for assuring security is made when a document is transmitted, image data is encrypted in a case where the document is transmitted by an electronic-mail 10 function, and the above-mentioned private security function is used, if possible, in a case where the document is transmitted by facsimile.

As many apparently widely different embodiments of the present invention can be made without departing from 15 the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.